UNC CHARLOTTE
The WILLIAM STATES LEE COLLEGE of ENGINEERING
Industrial Solutions Laboratory

Company Information

Company Name	*Electric Power Research Institute (EPRI)*	**Date Submitted**	*05/03/2021*
Project Title	Cyber Security Detection Using a Zeek Raspberry PI Sensor **(EPRI_ZEEK)**	**Planned Starting Semester**	*Fall 2021*

Senior Design Project Description

Personnel

Typical teams will have 4-6 students, with engineering disciplines assigned based on the anticipated Scope of the Project.

Please provide your estimate of staffing in the below table. The Senior Design Committee will adjust as appropriate based on scope and discipline skills:

Discipline	**Number**	**Discipline**	**Number**
Mechanical		Electrical	2
Computer	3	Systems	
Other ( )			

Company and Project Overview:

The Electric Power Research Institute (EPRI) conducts research, development, and demonstration projects for the benefit of the public in the United States and internationally. As an independent, nonprofit organization for public interest energy and environmental research, we focus on electricity generation, delivery, and use in collaboration with the electricity sector, its stakeholders and others to enhance the quality of life by making electric power safe, reliable, affordable, and environmentally responsible.

EPRI has collaborated with the electricity sector and its stakeholders since 1972 and our membership has grown to represent approximately 90% of the electric utility revenue generated in the United States and extends to participation in more than 38 countries. The worldwide membership that supports our work comprises more than 1,000 organizations. While most members are electric utilities, others are businesses, government agencies, regulators and public or private entities engaged in some aspect of the generation, delivery, or use of electricity. Through their advisory roles in EPRI, its research sectors and programs, EPRI members help inform the development of EPRI's annual research portfolio, identify critical and emerging electricity industry issues, and support the application and technology transfer of EPRI's research and development.

Cyber intrusion detection in industrial controls is crucial in mitigating cyber security risks to operations and safety. An intrusion detection system (IDS) monitors network traffic for anomalies at various points in the network. The IDS monitors for unusual network behavior as well as indications of malicious activity and then creates logs of the events and sends alerts to cyber security incident responders. The network traffic logs can then be sent to a security suite that collects aggregate logs for further analysis. The logs are also analyzed by security personnel to determine if an incident has occurred. EPRI is performing research into analytic solutions of this network traffic for cyber and operational detection.

Project Requirements:

This project seeks to develop a solution using commonly available open-source and low-cost software and hardware. Zeek (formerly BRO) is an open-source traffic capture and anomaly detection software that is widely used.

Traffic is observed using a SPAN port or network TAP and passed to a network sensor. The network sensor is typically a workstation or server configured to capture and analyze traffic. The project will first establish the representative network architecture and then identify the number of sensors and locations for optimal visibility. The network architecture will be similar to that seen in industrial control systems networks.

The project will then configure Zeek sensors using Raspberry PI's (or similar readily available hardware) for network traffic analysis for later instrumentation and control lab research. The project will the Raspberry Pi sensors using security best practices, and install and configure Zeek for network traffic analysis. Sample network data will be provided in the form of packet capture (PCAP) files to test the functionality of the solution.

Expected Deliverables/Results:

- Design a network architecture and configuration required for network visibility across an OT network.
- A configured Raspberry PI, with security hardening best practices documented and implemented. The Raspberry PI will be configured to analyze data from the representative architecture using Zeek.
- Zeek must be configured to create alerts and capture log files when specific conditions occur, provided by the project mentor. Zeek will also be configured to perform pre-processing of the raw network information and generate metadata that can be used for later analysis.
- Verification testing using provided open-source PCAP data with known security events.

Disposition of Deliverables at the End of the Project:

The prototype system and a technical write-up of the system would be demonstrated at the Expo and transitioned to EPRI after the conclusion of the Expo.

List here any specific skills, requirements, specific courses, knowledge needed or suggested (If none please state none):

- Interest in network architecture and security systems.